Private Connections: Unique Privacy Provisions for a Neurodiverse Community

Phil Fox
foxp2@wwu.edu

Artem Dukhnitskiy
dukhnia@wwu.edu

Michail Tsikerdekis
Michael.Tsikerdekis@wwu.edu

Shameem Ahmed
ahmeds@wwu.edu

Department of Computer Science
Western Washington University
Bellingham, WA

1. INTRODUCTION

Dating applications popularly make use of Location Based Services (LBS), Facebook-facilitated registration/log-ins, and 'binary' connected/non-connected visibility for profile information [8, 9]. Even if the above features are wholly appropriate on their existing platforms, are they appropriate for future platforms? Can certain online communities benefit from either the absence of the above features or more robust implementations?

Western Washington University's *Connection* mobile application is an in-development dating and friendship facilitating platform tailored towards users who either self-identify or are diagnosed as *Neurodiverse*. Neurodiverse populations are also referred to as affected by Autism Spectrum Disorder or Asperger's Syndrome.

Connection aims to create an online space wherein Neurodiverse users can facilitate beneficial relationships through features that focus on users' interests and enable expressive communication which may not be available on other social/dating platforms [7].

Current research shows that Neurodiverse community members consider repercussions such as being misunderstood, cyberbullying, and unwanted special treatment when deciding to disclose/not-to-disclose their Neurodiverse status [2].

Connection is an inclusive platform by-design, and our analysis yields privacy implementations which aim to give Neurodiverse users robust control over profile visibility and minimize risk of unwanted Neurodiverse status disclosures to the outside world.

2. RELATED WORK

Sedgewick, Hill, and Pelicano show that social media interactions "Serve to reinforce offline friendships" for some Neurodiverse users. These interactions can serve as support for a phenomena called 'camoflauging' or 'masking' in which (prominently female) Neurodiverse adolescents and adults "conciously 'mask' the diagnostic features of autism to fit in with Neurotypical peers". [12]

A series of studies have investigated existing privacy control mechanisms. We present some of these in this section as a means for providing an overall context in the applications of such mechanisms. These are not meant to be exhaustive but representative of the current domain.

Misra and Such investigate privacy/access controls across 30 social media sites and identified pros and cons of specific implementations. They note that there are three 'main' classes of privacy access controls and highlight concerns on privacy controls' lack of dynamic response to user sharing. [9].

Mata et al. aggregate studies of over 30 dating and social media apps and identified recoverable artifacts from 12 applications that either disclosed users' personal information, Facebook profiles, private files, or estimated geographic locations [8].

Both Huang et al. and Hoang et al. show relevant concerns over exploitable weaknesses in current LBS models in dating apps [6, 4]. Both Hong et al. and Burke et al. outline individual concerns regarding online privacy from Neurodiverse interview participants [2, 5]. Hong et al. in particular propose the concept of *SocialMirror*, a specialized social network built to facilitate quality of daily life features for Neurodiverse users [5].

3. METHODOLOGY

Our proposal is based on an analysis of 43 peer reviewed articles and conference proceedings from journals *Autism*, *Focus On Autism and Other Developmental Disabilities*, the ACM Digital Library, and IEEE Xplore. The findings are based a review of a systematic keyword-based search was performed on the prior databases in April and May 2019. Figure 1 presents the search strings used based on the journals in which they are performed.

Autism, Focus On Autism...
dating **AND** (priva* **OR** secur*) **AND**
(internet **OR** online)

IEEE Xplore, ACM Library
I: (autis* **OR** asperger*) **AND** (priva* **OR** secur*)
II: dating **AND** (priva* OR secur*) **AND**
(online **OR** relati* **OR** app)

Figure 1: Search strings used to collect research articles

The above asterisk (*) after a keyword represents words beginning with that particular substring. Since the IEEE Xplore database did not offer an asterisk-operator, the disjunctive criteria instead included the strings '(privacy OR private OR security OR secure)', '(asperger OR asperger's)' and the full phrase 'relationship'. Combinations of the above key terms were used to extract as many relevant articles as possible. Currently, the above search strings yield 486 articles. Inconsistencies are noticed in all four databases wherein constrained searches aiming at yielding fewer than 100 results often badly undercount relevant articles. Full-text and less constrained searches capture a majority of relevant articles but yield between 500 and 15,000 results per string. In several instances, articles *not* containing *any* instances of phrase 'dating' (to include ' "dating" ') and others including 'updating' and 'validating' are returned, obscuring relevant results.

Our starting goal is first isolating articles pertaining to both relevant general (i.e. corporeal or non-online) and online privacy concerns of Neurodiverse populations. Next, we compile privacy concerns regarding dating/social media platforms along with studying pros and cons of particular existing privacy implementations for dating/social media applications. Lastly, support is added, where necessary, to connect any non-overlapping general privacy concerns of Neurodiverse populations to their counterpart worries regarding online platforms.

For reinforcement, interviews with at least 20 Neurodiverse and Neurotypical participants/app testers are in progress by the *Connection* development team. Two relevant questions are posed in the interest of this paper: 1) "What types of personal information are you comfortable publicly identifying with on social platforms (e.g. real name, age, city of residence, etc.)?" and 2) "What types of personal information, if required to post publicly, would discourage you from using a social platform?" Responses to these questions illuminate means in which the *Connection* platform will be maximally attractive to users, while highlighting privacy concerns unique to Neurodiverse users wherein Neurotypical participants' responses are considered as a control.

Citation lists from each search were compiled in a Mendeley database where duplicate articles (4) were removed and the exclusion process followed. A significant portion of the results pertained to Neurodiverse communities on the basis of medical treatment, screening, intervention, parents of Neurodiverse diagnosees, or focused exclusively children (less than adolescent age). The *Connection* platform does not intend to implement medical, screening, or intervention protocols, and is tailored towards a mainly adult audience so studies and conference proceedings of these natures were excluded.

Exclusion criteria regarding ACM and IEEE Xplore databases ignore articles that pertain to insider/3rd-party access (database, development, etc.), social media advertising/marketing schema, and payment or financial considerations for the following reasons: One, 'insider' threats are outside the *current* scope of this study since Connections is in an early development and controlled deployment phase; user-to-user privacy concerns are paramount. Second, there are no near or long-term plans to either include third-party support or develop *Connections* as a pay-for-use/feature platform. Third, based on an initial stage of this review (Neurodiverse-specific searches), 'second-party' threats (e.g. other platform users) are ones in which pose a particular increased concern to the privacy of Neurodiverse users.

4. FINDINGS AND IMPLEMENTATIONS

The findings from our literature review show that 'camouflaging' and 'masking' are synonymous terms and are widely accounted for phenomena for (high-functioning) Neurodiverse social behaviors in adolescents and young adults. [12, 3]. Other research shows that Neurodiverse online users face being taken advantage of or manipulated [1]. Lastly, reported instances of offline bullying and harassment are markedly skewed towards male adolescent Neurodiverse populations when compared to Neurotypical [10]. It is not surprising that online interactions for Neurodiverse can serve to reinforce offline relationships [12], but *Connection* needs to be adequately flexible to be useful in generating *new* relationships between its members.

How can *Connection* both 'connect' users on the basis of shared identification as members of Neurodiverse communities while not disclosing members' statuses in an unwanted way? In the worst-case, either our privacy implementations make potential *Connection* users uncomfortable participating on our platform, or the privacy controls seem to users as if they're more trouble than they're worth. We intend to avoid both these cases by a wide berth. Given the above findings and our commitment to inclusivity, it is reasonable to impose the following design implementations and constraints on the *Connection* app:

4.1 Connections' Membership

A natural way to avoid unwanted disclosure of Neurodiverse users' status is to generalize the user Neurodiverse/typical population. This is achieved by recruiting and adding attractive features that successfully encourage *Neurotypical* users to become active *Connection* members yielding the following benefit: An outside out-of-network user will have no reliable way to determine a user's Neurodiverse status merely by a user's participation on the *Connection* platform. All the better, *Connection* maintains it's goals in inclusivity in doing so. These considerations propose a high-level challenge for *Connection's* developers: It is necessary to generate a platform that can compete with other high-level dating/social media platforms. Success in this endeavor is highly contingent on keeping pace with the greater (growing) market of similar applications which attract Neruotypical users' finite time spent on these types of platforms.

4.2 Visibility and Registration Implementa -tion

Privacy control implementation on social media platforms are shown to range from 'public-only' and binary (sparse) visibility controls to user-defined or preset visibility control-groups (robust). Sparse visibility controls offer merely a binary distinction, which affects what content unauthorized users can see [8]. Put simply, a user elects to have a public and private profile and a single authorization provides other users with access to one's private profile that includes any information that was decided to be disclosed there. Popular instances of 'public-only' privacy controls are non-protected user profiles in YouTube and most internet forums. Binary controls are/were seen in MySpace and Pintrest. LinkedIn and Google+ use defined groups, preset and user-defined respectively [9].

A robust implementation of visibility controls is particularly relevant for the *Connection* platform. Given that *Connection* is both friendship and intimate relationship-facilitating by design, users naturally have information that is appropriate for sharing in one venue which is not always appropriate for the other. Taking Facebook as an example, users who have both close friends and family members may opt to display and restrict posts on certain topics toward each group. Such is the case for *Connection*, perhaps to a more intimate extreme.

We propose that users self-define both the total number and particular content-restrictions of visibility groups. These restrictions should include access to users' real names, general locations, educational affiliation, uploaded photographs, etc. Further, we propose that 'splash-screen' privacy reminders and recommendations are offered to users to help detect when shared content might be a mismatch with the target audience. The detriment of this function adds some 'cognitive overhead' which makes the general user experience more complicated [8]. This can be mitigated by allowing users to freely choose sparse or robust privacy controls at their preference. The benefit of users being able to (comfortably) facilitate both friendly and more intimate relationships *without* creating more than one profile per user outweighs this detriment.

One worry about the above protocol is that *Connection* would be *de facto* encouraging anonymity between user communication. Anonymitized communications on platforms such as 4chan and Tor might be used to facilitate illegal activity [13] or serve as a vehicle for online harassment or bullying. Indeed, to an out-of-network outsider, Connection might appear *outwardly* like one of such websites at its users' preference. However, registration protocols for *Connection* must implement a system which verifies actual identities to platform administration and limiting accounts to one per verified user. In this way, harassing users can be held accountable unlike anonymitized platforms, and *Connections* users can freely disclose their more personal details in an optimally controlled way. This is a more strict implementation than other social media and dating platforms, but it stands to hold the *Connection* user-community accountable and safeguard its users at the same time. One popular means of obtaining reliable user-registration is through a Facebook registration portal. This method is too defective for our purposes (having more than one Facebook account is common) and leads to further user-vulnerabilities discussed in §5.2.

5. IMPLEMENTATIONS TO AVOID

LBS are useful for social media and dating application to show an estimate of distance between users, often in miles or kilometer units. Note that platforms which attempt to facilitate in-person meetings between users, often strangers, stand to gain the most from these features [11]. These services were shown as subject to *trilateration*, a process where an exploiting user can triangulate the location of a targeted user by observing changes in a 'distance-from' calculation. Trilateration was achievable on at least one platform even when the targeted user's LBS functionality was set as 'disabled' [6, 8].

Certain platforms that offer Facebook-connected login, registration, or verification were shown to lead an exploiting user from said platforms back to targeted users' Facebook accounts. Facebook connectivity facilitates user verification and brief registration processes under optimal conditions. Facebook tokens disclosing either FacebookIDs or users' actual names were recovered on device virtual drives and shown as accesible by researchers. This discovery process was possible after exchanging messages with a target user in at least one case [8].

5.1 LBS Implementation

The vulnerability and potential unreliability of LBS-disabling options shown above gives us enough pause to restrict this functionality in *Connection*. Instead, users may opt to provide self-report their zip code for a generalized location in lieu of using LBS. The detriment of this function is that users must update this information manually if relocating, and some users will opt to provide no information or false information. The benefit of removing the possibility of LBS trilateration from exploiting users outweighs the previous detriment on behalf of users' safety and relative anonymity.

5.2 Facebook Connectivity

Facebook connectivity or verification should be avoided for this particular platform. It is reasonable to expect that some *Connection* users wish to share online information within *Connection* which is purposefully excluded from said user's Facebook profile and vice versa. The detriment of this restriction is a loss of a virtual 'one-click' registration feature for users, and a semi-reliable verification that a user is real and using only one *Connection* account. The benefit of better preserving *Connection* users' personal data and defending it from attack outweighs this detriment. It is safe to assume that certain *Connection* users wish to avoid public disclosure of their membership in Neurodiverse communities, wherein a successful attack would be tantamount to 'outing' these users', or making them vulnerable to doxing or harassment.

6. DISCUSSION

A primary limitation of our literature review is the lack of systematicity in the searching approach of ACM and IEEE Xplore databases. The inclusion of often thousands of false-positive search results for effective searches limits our ability

to comprehensively review the breadth of possibly relevant articles to our project. Including further support puts our project at-risk of appearing to 'cherry-pick' or give special consideration to some articles and not others in a biased way. Additionally, other articles may exist outside of this project's scope that deny the above observations or findings.

A secondary limitation of our study is that *Connection* might potentially include payment, third-party design implementation, or significant management change in the future. Should this be the case, the scope of this review should consider expansion regarding specific implementations on tracking features like cookies, IP address management, cache controls, and more to remain appropriately comprehensive. Privacy concerns from users are often 'high-level' regarding how *corporations* handle personal data and information. The focus on 'second-party' threats in this literature review does not preclude future work on how best to protect user data in general. However, we do not have reason to believe that Neurodiverse communities are at any particular greater risk from corporate and third-party privacy threats than Neurotypical communities at this time.

7. CONCLUSION

We have shown that the benefits of implementation and restriction of particular features outweigh the associated detriments regarding the *Connection* platform currently in development. Even under the assumption that sparse profile visibility, LBS features, and Facebook connectivity are appropriate implementations for their respective platforms, our reasoning holds for our unique platform, tailored for a unique community.

8. REFERENCES

[1] G. P. Barnhill. Outcomes in Adults With Asperger Syndrome. *Focus on Autism and Other Developmental Disabilities*, 22(2):116–126, may 2007.

[2] M. Burke, R. Kraut, and D. Williams. Social use of computer-mediated communication by adults on the autism spectrum. In *Proceedings of the 2010 ACM Conference on Computer Supported Cooperative Work*, CSCW '10, pages 425–434, New York, NY, USA, 2010. ACM.

[3] S. Cribb, L. Kenny, and E. Pellicano. 'I definitely feel more in control of my life': The perspectives of young autistic people and their parents on emerging adulthood. *Autism*, pages 1362–3613, Feb 2019.

[4] N. P. Hoang, Y. Asano, and M. Yoshikawa. Your neighbors are my spies: Location and other privacy concerns in glbt-focused location-based dating applications. In *2017 19th International Conference on Advanced Communication Technology (ICACT)*, pages 851–860, Feb 2017.

[5] H. Hong, J. G. Kim, G. D. Abowd, and R. I. Arriaga. Designing a social network to support the independence of young adults with autism. In *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work*, CSCW '12, pages 627–636, New York, NY, USA, 2012. ACM.

[6] R. Huang, Y. Lin, B. Ying, and A. Nayak. Acp: An efficient user location privacy preserving protocol for opportunistic mobile social networks. *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, 01:610–619, 2018.

[7] C. Johnson and M. Sharmin. Connection: An autism-focused dating app. In *Grace Hopper 2018 Poster Submission*, GHC '18, pages 1–3, Bellingham, WA, USA, 2018.

[8] N. Mata, N. Beebe, and K.-K. R. Choo. Are your neighbors swingers or kinksters? feeld app forensic analysis. *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pages 1433–1439, 2018.

[9] G. Misra and J. M. Such. How socially aware are social media privacy controls? *Social Computing*, 49(3):96–99, March 2016.

[10] K. P. Nowell, C. M. Brewton, and R. P. Goin-Kochel. A Multi-Rater Study on Being Teased Among Children/Adolescents With Autism Spectrum Disorder (ASD) and Their Typically Developing Siblings: Associations With ASD Symptoms. *Focus on Autism and Other Developmental Disabilities*, 29(4):195–205, feb 2014.

[11] B. Obada-Obieh and A. Somayaji. Can i believe you?: Establishing trust in computer mediated introductions. In *Proceedings of the 2017 New Security Paradigms Workshop*, NSPW 2017, pages 94–106, New York, NY, USA, 2017. ACM.

[12] F. Sedgewick, V. Hill, and E. Pellicano. 'It's different for girls': Gender differences in the friendships and conflict of autistic and neurotypical adolescents. *Autism*, pages 1362–3613, Oct 2018.

[13] M. Spitters, S. Verbruggen, and M. v. Staalduinen. Towards a Comprehensive Insight into the Thematic Organization of the Tor Hidden Services. In *2014 IEEE Joint Intelligence and Security Informatics Conference*, pages 220–223, 2014.